IN THE CLAIMS

Please amend the claims as follows:

Claim 1 (Currently Amended): An encryption processing apparatus configured to perform a data encryption process, said encryption processing apparatus comprising:

a control section configured to set a mixed encryption processing sequence by dividing an original encryption processing sequence into a plurality of groups composed of one or more encryption processing units, each group being a separate and independent encryption process for encrypting an input data, where the input data to be encrypted for one of the groups is different and generated independently relative to ~~than~~ the input data to be encrypted for ~~the other~~ another one of the groups, said control section mixing processing sequences of encryption processing units of the plurality of groups with each other by inserting at least one encryption processing unit from one of the groups between encryption processing units from another one of the groups so that performance of at least one ~~process~~ encryption processing unit from one of the groups is performed at a time between ~~processes~~ performance of encryption processing units from another one of the groups and under a condition in which a processing sequence of the encryption processing units within each of the plurality of groups is fixed; and

an encryption processing section configured to perform an encryption process in accordance with the mixed encryption processing sequence set by said control section.

Claim 2 (Previously Presented): An encryption processing apparatus according to Claim 1, wherein each group includes a triple-DES encryption process and said control section is configured to set a dummy single-DES process as a dummy encryption process that is unnecessary for an encryption processing sequence in at least one of said groups, and set the number of dummy single-DES processes to be a multiple of 3, and wherein said control

section is configured to set a dummy encryption processing unit that performs the dummy encryption process in at least one of the groups, and set one mixed encryption processing sequence by mixing the encryption processing units of a plurality of groups containing the dummy encryption processing unit.

Claim 3 (Previously Presented): An encryption processing apparatus according to Claim 1, wherein said control section is configured to determine a group of sequences, which can be performed independently of each other, within the original encryption processing sequence to be divided in a process of division into the plurality of groups, and perform a process for setting a group of divisions in which each of the sequences in the group of sequences can be performed independently as a unit.

Claim 4 (Previously Presented): An encryption processing apparatus according to Claim 1, wherein said encryption processing unit is a single-DES encryption process, and

wherein said control section is configured to set the mixed encryption processing sequence by dividing the original encryption processing sequence containing one or more single-DES encryption processes into a plurality of groups composed of one or more single-DES encryption processes and by mixing the single-DES encryption processing units contained in each group by mutual replacement of the single-DES encryption processing units of each set group under the condition in which the processing sequence within each set group is fixed.

Claim 5 (Previously Presented): An encryption processing apparatus according to Claim 1, wherein said control section is configured to perform a process for dividing the encryption processing sequence into a plurality of groups composed of one or more

encryption processing units by using a single-DES encryption process which forms a triple-DES encryption process as an encryption processing unit.

Claim 6 (Previously Presented): An encryption processing apparatus according to Claim 1, wherein the original encryption processing sequence to be mixed is an encryption processing sequence including a random-number generation process, and

said control section is configured to form a random-number generation process as a process including a conversion process by three single-DES processes, and sets the three single-DES processes as a random-number generation process in one of the groups of divisions.

Claim 7 (Canceled).

Claim 8 (Previously Presented): An encryption processing apparatus according to Claim 1, wherein said encryption processing apparatus has a memory for storing processing results of the encryption processing units which form the mixed encryption processing sequence set by said control section, and

said control section is configured to store the processing results in said memory in such a manner as to be capable of identifying which encryption processing unit the processing results are obtained from.

Claim 9 (Currently Amended): An encryption processing apparatus configured to perform a data encryption process, said encryption processing apparatus comprising:

a control section configured to set a mixed encryption processing sequence by dividing an original encryption processing sequence into a plurality of groups which include

one or more encryption processing units, each group being a separate and independent encryption process for encrypting an input data, where the input data to be encrypted for one of the groups is different and generated independently relative to ~~than~~ the input data to be encrypted for ~~the other~~ another one of the groups, said control section adding dummy encryption processing units as encryption processing units to at least one of the groups that performs dummy encryption processes that are unnecessary for the original encryption processing sequence, and said control section performing a mixing of processing sequences of the encryption processing units of the plurality of groups with each other by inserting at least one encryption processing unit from one of the groups between encryption processing units from another one of the groups so that performance of at least one ~~process~~ encryption processing unit from one of the groups is performed at a time between ~~processes~~ performance of encryption processing units from another one of the groups; and

an encryption processing section configured to perform an encryption process in accordance with the mixed encryption processing sequence set by said control section.

Claim 10 (Previously Presented): An encryption processing apparatus according to Claim 9, wherein an encryption processing unit contained in said original encryption processing sequence is a single-DES encryption process,

said control section is configured to set said dummy encryption processes as single-DES encryption processes and

wherein said control section is configured to set the number of dummy encryption processes to a multiple of 3.

Claim 11 (Currently Amended): An encryption processing method for performing a data encryption process, said encryption processing method comprising:

dividing an original encryption processing sequence into a plurality of groups composed of one or more encryption processing units, each group being a separate and independent encryption process for encrypting an input data, where the input data to be encrypted for one of the groups is different and generated independently relative to ~~than~~ the input data to be encrypted for ~~the other~~ another one of the groups;

setting a mixed encryption processing sequence by mixing processing sequences of encryption processing units of the plurality of groups with each other by inserting at least one encryption processing unit from one of the groups between encryption processing units from another one of the groups so that performance of at least one ~~process~~ encryption processing unit from one of the groups is performed at a time between ~~processes~~ performance of encryption processing units from another one of the groups and under a condition in which a processing sequence of the encryption processing units, set in said dividing, within each group is fixed; and

performing an encryption process in accordance with the mixed encryption processing sequence set in said setting.

Claim 12 (Previously Presented): An encryption processing method according to Claim 11, wherein each group includes a triple-DES encryption process and said dividing includes setting a dummy single-DES process as a dummy encryption process that is unnecessary for the original encryption processing sequence in at least one of said groups, and setting the number of single-DES processes of dummies to be set to a multiple of 3, said method further comprising:

setting a dummy encryption processing unit that performs the dummy encryption process in at least one of the groups, and

setting the mixed encryption processing sequence by mixing the encryption processing units of a plurality of groups containing said dummy encryption processing units.

Claim 13 (Previously Presented): An encryption processing method according to Claim 11, wherein said dividing determines a group of sequences, which can be performed independently of each other, within the original encryption processing sequence to be divided in a process of division into the plurality of groups, and performs a process for setting a group of divisions in which each of the sequences in the group of sequences can be performed independently as a unit.

Claim 14 (Previously Presented): An encryption processing method according to Claim 11, wherein each of said encryption processing units is a single-DES encryption process,

said dividing divides the original encryption processing sequence containing one or more single-DES encryption processes into a plurality of groups composed of one or more single-DES encryption processes, and

said setting sets one mixed encryption processing sequence by mixing the single-DES encryption processing units contained in each group by mutual replacement of the single-DES encryption processing units of each set group under the condition in which the processing sequence within each set group is fixed.

Claim 15 (Previously Presented): An encryption processing method according to Claim 11, wherein

said dividing performs a process for dividing the encryption processing sequence into a plurality of groups composed of one or more encryption processing units with a single-DES

encryption process which forms a triple-DES encryption process being an encryption processing unit.

Claim 16 (Previously Presented): An encryption processing method according to Claim 11, wherein the original encryption processing sequence to be mixed is an encryption processing sequence including a random-number generation process, and

said encryption processing method further comprises forming a random-number generation process as a process including a conversion process by three single-DES processes and setting the three single-DES processes as a random-number generation process in one of the groups.

Claim 17 (Canceled).

Claim 18 (Previously Presented): An encryption processing method according to Claim 11, further comprising:

storing processing results in a memory for storing processing results of the encryption processing units which form the mixed encryption processing sequence in such a manner as to be capable of identifying which encryption processing unit the processing results are obtained from.

Claim 19 (Currently Amended): An encryption processing method for performing a data encryption process, said encryption processing method comprising:

dividing an original encryption processing sequence, into a plurality of groups which include one or more encryption processing units, each group being a separate and independent encryption process for encrypting an input data, where the input data to be

encrypted for one of the groups is different and generated independently relative to ~~than~~ the input data to be encrypted for ~~the other~~ another one of the groups,

setting a mixed encryption processing sequence by adding dummy encryption processing units as encryption processing units to at least one of the groups, the dummy encryption processing units performing dummy encryption processes that are unnecessary for the original processing sequence and by mixing processing sequences of the encryption processing units of the plurality of groups with each other by inserting at least one encryption processing unit from one of the groups between encryption processing units from another one of the groups so that performance of at least one ~~process~~ encryption processing unit from one of the groups is performed at a time between ~~processes~~ performance of encryption processing units from another one of the groups; and

performing an encryption process in accordance with said mixed encryption processing sequence.

Claim 20 (Previously Presented): An encryption processing method according to Claim 19, wherein an encryption processing unit contained in said original encryption processing sequence is a single-DES encryption process,

said setting sets said dummy encryption processes as a single-DES encryption process, and

wherein said dividing includes setting the number of dummy encryption processes to a multiple of 3.

Claim 21 (Currently Amended): A computer readable storage medium encoded with computer executable instructions, which when executed by a computer, cause the computer to perform a method comprising:

dividing an original encryption processing sequence into a plurality of groups composed of one or more encryption processing units, each group being a separate and independent encryption process for encrypting an input data, where the input data to be encrypted for one of the groups is different and generated independently relative to ~~than~~ the input data to be encrypted for ~~the other~~ another one of the groups;

setting a mixed encryption processing sequence by mixing processing sequences of encryption processing units of the plurality of groups with each other by inserting at least one encryption processing unit from one of the groups between encryption processing units from another one of the groups so that performance of at least one ~~process~~ encryption processing unit from one of the groups is performed at a time between ~~processes~~ performance of encryption processing units from another one of the groups and under a condition in which a processing sequence of the encryption processing units, set in said dividing, within each group is fixed; and

performing an encryption process in accordance with the mixed encryption processing sequence set in said setting.

Claim 22 (Currently Amended): A computer readable storage medium encoded with computer executable instructions, which when executed by a computer, cause the computer to perform a method comprising:

dividing an original encryption processing sequence, into a plurality of groups which include one or more encryption processing units, each group being a separate and independent encryption process for encrypting an input data, where the input data to be encrypted for one of the groups is different and generated independently relative to ~~than~~ the input data to be encrypted for ~~the other~~ another one of the groups

setting a mixed encryption processing sequence by adding dummy encryption processing units as encryption processing units to at least one of the groups, the dummy encryption processing units performing dummy encryption processes that are unnecessary for the original processing sequence and by mixing processing sequences of the encryption processing units of the plurality of groups with each other by inserting at least one encryption processing unit from one of the groups between encryption processing units from another one of the groups so that performance of at least one ~~process~~ encryption processing unit from one of the groups is performed at a time between ~~processes~~ performance of encryption processing units from another one of the groups; and

performing an encryption process in accordance with said mixed encryption processing sequence.